TURBIN CHU HEIDT, A Law Corporation
Richard Turbin (1044)
richturbin@turbin.net
Janice D. Heidt (8984)
jheidt@turbin.net
737 Bishop Street, Suite 2730
Honolulu, Hawaii 96813
Telephone: 808-528-4000
Facsimile: 808-599-1984

SCHUBERT JONCKHEER & KOLBE LLP
Amber L. Schubert
aschubert@sjk.law.com
2001 Union St., Ste. 200
San Francisco, CA 94123
Tel: (415) 788-4220
Fax: (415) 788-0161

Attorneys for Plaintiffs RANDEE ARKIN and
DOMINIC RAMISCAL and the Proposed Class

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF HAWAII

RANDEE ARKIN and DOMINIC RAMISCAL *Plaintiffs*, v. HAWAII RADIOLOGIC ASSOCIATES, LTD., *Defendant*.	CIVIL NO. _____ (Other Personal Injury) **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs RANDEE ARKIN and DOMINIC RAMISCAL (hereinafter "Plaintiffs," or "ARKIN" and "RAMISCAL," respectively), on behalf of themselves and all others similarly situated, allege the following complaint against Defendant HAWAII RADIOLOGIC ASSOCIATES, LTD. (hereinafter "HAWAII RADIOLOGIC" or "Defendant") upon personal knowledge as to their own acts, and based upon their investigation, their counsel's investigation, and information and belief as to all other matters.

NATURE OF THE CASE

1. This is a Class Action to recover damages sustained and suffered by Plaintiffs, on behalf of themselves and all others similarly situated, caused by a) Defendant's negligent failure to implement adequate security measures to protect the confidentiality of patient health information and other personal information, and b) Defendant's negligent and unreasonable delay in notifying victims after Defendant learned unauthorized parties had hacked its computer systems and accessed the HAWAII RADIOLOGIC computer network, including all patient PII (Personal Identifying Information) and PHI (Personal Health Information), all of which encompassed an extreme degree of highly sensitive information.

2. Plaintiffs, as individuals and on behalf of all others similarly situated, allege claims of Negligence, Breach of Implied Contract, and Unjust Enrichment.

3. Plaintiffs, as individuals and on behalf of all others similarly situated, further ask the Court to compel Defendant to adopt reasonable information security practices to secure the sensitive PHI and PII that Defendant collects and stores in its databases and to grant such other relief as the Court deems just and proper.

PARTIES

Plaintiffs

4. Plaintiff RANDEE ARKIN is a natural person and a resident and citizen of Keeau, Hawai‘i, who used Defendant HAWAII RADIOLOGIC’s services. On or around November 5, 2024, she received a notice from Defendant informing her that her PII (Personal Identifying Information) and PHI (Personal Health Information) had been breached.

5. Plaintiff DOMINIC RAMISCAL is a natural person and a resident and citizen of Mountain View, Hawai‘i, who used Defendant’s HAWAII RADIOLOGIC’s services. On or around November 5, 2024 he received a notice from Defendant informing him that his PII (Personal Identifying Information) and PHI (Personal Health Information) had been breached.

Defendant

6. Defendant HAWAII RADIOLOGIC ASSOCIATES, LTD., is a healthcare services group that provides diagnostic radiologic imagining at three

imaging centers located in the Island of Hawai‘i, (colloquially, the “Big Island”). It is organized and exists under the laws of the State of Hawai‘i. It has its administrative office located at 688 Kinoole St., Ste 103, Hilo, Hawai‘i 96720, and all its clinics and imaging centers are located at various sites on the Island of Hawai‘i.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction and diversity jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The class contains more than 100 members (indeed, the U.S. Department of Health and Human Services identified that more than 23,205 people were impacted), and many of these members have citizenship diverse from HAWAII RADIOLOGIC.[1]

8. HAWAII RADIOLOGIC’s data breach notice provided information for putative class members who are citizens of Maryland, New Mexico, New York, North Carolina, and Rhode Island. Indeed, Defendant’s Data Breach notice letter acknowledged that “[t]here are approximately 3 Rhode Island residents that may be impacted by this event.” In light of the transient nature of many Hawai’i

[1]Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, https://www.google.com/search?q=hawaii+radiologic+data+breach+number+of+people+mpacted&rlz=1C5CHFA_enUS965US965&oq=hawaii+radiologic+data+breach+number+of+people+mpacted&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBCDY2MTJqMGo3qAIAsAIA&sourceid=chrome&ie=UTF-8, (last visited November 23, 2024).

residents and the substantial number of visitors the island received during the Class Period, on information and belief, a substantial portion of the putative class is composed of citizens of others states.[2]

9. The exercise of personal jurisdiction over HAWAII RADIOLOGIC is appropriate as its headquartered in the State of Hawai'i and conducts substantial business in the State of Hawai'i.

10. Venue is proper in the District of Hawai'i under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because a substantial part of the events giving rise to the claims emanated from activities within the State of Hawaii, and HAWAII RADIOLOGIC is headquartered and conducts business in the State of Hawai'i.

FACTUAL ALLEGATIONS

I. Background: Defendant Stores a Huge Amount of PII, including Class Members'

11. Defendant HAWAII RADIOLOGIC is a healthcare group that provides radiologic imaging services to medical patients at three imaging centers located on the Island of Hawaii.

[2] *See* State of Hawai'i, Department of Business, Economic Development & Tourism, 2023 Annual Visitor Research Report, https://www.hawaiitourismauthority.org/media/13190/2023-annual-report-final.pdf at 13 (last visited Nov. 6, 2024) .

12. Plaintiff and members of the Plaintiff Class are former or current patients who used HAWAII RADIOLOGIC's services.

13. In order to receive treatment, Plaintiff and class members were required to provide all or part of the following non-exclusive list of sensitive PHI and PII during the regular course of business:

- Full name and mailing or personal address
- Social Security Number
- Date of Birth
- Driver's License Number
- State ID Number
- Passport Number,
- Financial Account/Bank Account Number
- Routing Number
- Bank Name
- Credit/Debit Card Number
- Card CVV and expiration date
- Security PIN/Security Code
- Login Information
- Medical Diagnosis Information
- Clinical Information
- Medical Treatment/Procedure Information
- Treatment Type,
- Treatment Location,
- Treatment Cost Information
- Doctor's Name

- Medical Record Numbers
- Patient Account Numbers
- Prescription information
- Biometric Data.

14. The above information is extremely sensitive personal identifying information and personal health information ("PII" and "PHI," respectively). This information is extremely valuable to criminals because it can be used to commit serious identity theft and medical identity theft crimes.

15. As a condition of doing business and obtaining the services of HAWAII RADIOLOGIC, class members entrusted HAWAII RADIOLOGIC with this information with the explicit and implicit understanding that the information would be kept secure and that reasonable measures would be taken to maintain and ensure the security, including timely notification in the event of a breach, commensurate with the value of data. This commitment to keeping patient data secure was noted on Defendant's website including its HIPAA notice.

II. The Breach

16. On or around November 5, 2024, Plaintiffs received a "Notice of Security Incident" letter from Defendant (the "Data Breach Letter").

17. According to the Data Breach Letter, on or around August 26, 2024, HAWAII RADIOLOGIC became aware of suspicious activity on its computer

network. However, an investigation conducted by the Defendant concluded that an unknown actor had gained access to its computer system as early as August 20, 2024. Consequently, the Defendant further concluded in its Data Breach Letter "the unknown actor may have had access to certain files within these systems and information may have been accessed or acquired."

18. Specifically, the information accessed or acquired included "name and date of birth, health insurance subscriber ID, types of exams, and indications for exams provided."

19. Although the Defendant uses evasive and ambiguous language throughout the Data Breach Letter, such as by stating the so-called security incident "may impact the privacy of [Plaintiffs'] personal information," and avers "[w]e have no evidence that this information has been subject to actual or attempted use," such language should not be construed as implying the Defendant does not have a reasonable belief that the PII and PHI of Plaintiffs and Class Members has been acquired without authorization by cybercriminals. Corporations only send such Data Breach Letters as was sent to Plaintiff in the instant case to those persons whose personal information the Defendant itself reasonably believes has been accessed or acquired by unauthorized individuals or entities. By sending the Data Breach Letter to Plaintiffs and similarly affected consumers, Defendant admits it has a reasonable belief that the PII and PHI of

Plaintiffs and Class Members were accessed or otherwise acquired by unauthorized individuals or entities—i.e., cybercriminals.

20. Additionally, the "Notice of Data Security Incident" that Defendant sent Plaintiffs and other similarly affected consumers, including Class Members, hardly constituted notice at all as Defendant's notice was untimely and intentionally obfuscated important and material facts about the Data breach.

21. Despite becoming aware of the Data Breach on or around August 26, 2024, Defendant inexplicably waited *over two months* until November 5, 2024 to send personal notice of the Data Breach to Plaintiffs and similarly affected consumers, including Class Members. This was time Plaintiffs and Class Members could have used to mitigate their own damages from the Data Breach.

22. Furthermore, in its "Notice of Security Incident," Defendant does not disclose all the material facts of the breach such as the identity of the cybercriminals who perpetrated the Data Breach, or the details of the cause or causes of the Data Breach.

23. These undisclosed facts are material to Plaintiff and Class Members who retain a vested interest in ensuring their PII and PHI remain protected. The insufficient disclosures in the Data Breach Letter constituted a separate and distinct harm from the Data Breach itself because it prevented Plaintiffs and Class Members from taking timely steps to mitigate their own damages.

Notwithstanding Defendant's intentional obfuscation of the material facts of the Data Breach, what can still be gleaned from the Data Breach Letter include the following facts:

(a) The Data Breach was the work of cybercriminals

(b) The cybercriminals infiltrated Defendant's computer systems and downloaded consumers' PII and PHI from those systems

(c) Once inside the Defendant's computer systems, the cybercriminals targeted Plaintiffs' and Class Members' PII and PHI for download and theft.

24. Despite Defendant's negligence in maintaining the data security of Plaintiffs' and Class Members' PII and PHI, Defendant offers absolutely no remedies to Plaintiffs or class members in the Data Breach Letter. Instead, the Data Breach Letter merely tells Plaintiffs and similarly affected consumers, including Class Members, "[w]e encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors." Such an "encouragement" completely fails to acknowledge the harms sustained by Plaintiffs and Class Members due to the Data Breach and offers cold comfort where just compensation is due. That is because, (as explained in more detail in sections below), the harms sustained by Plaintiffs and Class Members are potentially irreversible and could last for the remainder of their lifetimes as they

cannot control how the cybercriminals who have accessed their PII may continue to sell, or otherwise share, that data on black markets on Dark Web to other individuals and entities who may continue to use that information to commit frauds and identity theft against them.

25. Apart from resulting in a violation of data security, the Data Breach also led to a major disruption of HAWAII RADIOLOGIC services. For example, when HAWAII RADIOLOGIC first became aware of the Data Breach on or around August 26, 2024, it cancelled all radiologic imaging appointments for the upcoming month of September as a security precaution.[3] This resulted in delays in critical medical treatment for many HAWAII RADIOLOGIC patients, including Plaintiff RANDEE ARKIN, who had to cancel 3 important appointments with her surgeon due to delays in the delivery crucial radiologic images from HAWAII RADIOLOGIC. Such harms go beyond data security concerns and extend to the realm of medical concerns as is often the case when healthcare providers in particular are subject to a data breach.

26. In short, Defendant's failure to implement and maintain reasonable cybersecurity protocols and procedures constituted a negligent act and/or

[3]Marty Stempniak, "Cybersecurity incident forces radiology practice to cancel all appointments so far in September," RADIOLOGY BUSINESS, (Sep. 19, 2024), https://radiologybusiness.com/topics/health-it/enterprise-imaging/cybersecurity-incident-forces-radiology-practice-cancel-all-appointments-so-far-september.

omission that deleteriously compromised the data security of Plaintiffs and putative Class Members, which could potentially be irreversible and last for their respective lifetimes. Such harms include the diminution of the inherent monetary value of Plaintiffs' and Class Members' undisclosed PII, but also the time and money Plaintiffs and Class Members will have to spend to ameliorate the detrimental effects of having their PII disclosed online to cybercriminals, including and not limited to, closely monitoring their financial accounts and placing fraud alerts on all their financial accounts. In addition, in cases like this, where a healthcare provider is subject to a data breach, harms also include those caused by delays in vital medical treatment as a result of the Data Breach.

III. HAWAII RADIOLOGIC's Privacy Representations

27. HAWAII RADIOLOGIC acknowledges its legal and contractual obligations to protect its patients' sensitive PII and PHI. According to the Defendant's required Notice of Privacy Practices, HAWAII RADIOLOGIC stated: "We are required by law to maintain the privacy of your health information." In order to make sure that the PHI and PII is kept private, HAWAII RADIOLOGIC had an obligation to at minimum undertake reasonable measures to secure this extremely sensitive data and unequivocally communicate this to Plaintiffs and the class.

IV. HAWAII RADIOLOGIC Failed to Comply with Reasonable Cybersecurity Standards

28. At all times relevant to this Complaint, HAWAII RADIOLOGIC knew or should have known the significance and necessity of safeguarding its customers' PII and PHI, and the foreseeable consequences of a data breach. HAWAII RADIOLOGIC knew or should have known that because it collected and maintained the PII and PHI for a significant number of customers, a significant number of customers would be harmed by a breach of its systems. HAWAII RADIOLOGIC further knew due to the nature of its business as a health care services provider, that a data breach could potentially result in the release of deeply personal, sensitive, and costly information about its patients.

29. Because PII is so sensitive and cyberattacks have become a rising threat, the FTC has issued numerous guides for businesses holding sensitive PII and emphasized the importance of adequate data security practices. The FTC also stresses that appropriately safeguarding PII held by businesses should be factored into all business-related decision making.

30. An FTC Publication titled "Protecting Personal Information: A Guide for Business" lays out fundamental data security principles and standard practices

that businesses should implement to protect PII.[4] The guidelines highlight that businesses should (a) protect the personal customer information they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems.

31. The FTC also recommends businesses use an intrusion detection system, monitor all incoming traffic to the networks for unusual activity, monitor for large amounts of data being transmitted from their systems, and have a response plan prepared in the event of a breach.

32. The FTC also recommends that businesses limit access to sensitive PII, require complex passwords to be used on the networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures—a step that would have been particularly prudent in light of the methods used by the perpetrators in this case.

33. Businesses that do not comply with the basic protection of sensitive PII are facing enforcement actions brought by the FTC. Failure to employ reasonable and appropriate measures to protect against unauthorized access to

[4] Protecting Personal Information: A Guide for Business, FEDERAL TRADE COMMISSION, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business, (last accessed Nov. 6, 2024).

confidential consumer data is an unfair act or practice prohibited pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45.

34. Many states' unfair and deceptive trade practices statutes are similar to the FTC Act, and many states adopt the FTC's interpretations of what constitutes an unfair or deceptive trade practice.

35. HAWAII RADIOLOGIC knew or should have known of its obligation to implement appropriate measures to protect its customers' PII but failed to comply with the FTC's basic guidelines and other industry best practices, including the minimum standards set by the National Institute of Standards and Technology Cybersecurity Framework Version 1.1.[5]

36. Defendant's failure to employ reasonable measures to adequately safeguard against unauthorized access to PII constitutes an unfair act or practice as prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, as well as by state statutory analogs.

37. HAWAII RADIOLOGIC failed to use reasonable care in maintaining the privacy and security of Plaintiffs' and Class Members' PII and PHI. If HAWAII RADIOLOGIC had implemented adequate security measures, cybercriminals could never have accessed the PII of Plaintiffs and Class Members, and the Data Breach would have either been prevented in its entirety or

[5] https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf. (last accessed 11/27/2023)

have been much smaller in scope. For example, if HAWAII RADIOLOGIC had implemented adequate systems sequestering different types of sensitive data on different computers and allowed access on a need-based basis the data breach may have been much smaller in scope. Likewise, if HAWAII RADIOLOGIC had implemented adequate security systems it could have detected and stopped the intrusion long before it accessed sensitive information on **more than 23,205 patients**. There would almost never be a business need to access this information and the access attempt should have immediately raised alarms. Additionally, while we do not yet know the precise reasons for the breach, poor data security practices and lack of compartmentalization are common patterns in data breaches of this magnitude and sensitivity. Finally, once HAWAII RADIOLOGIC became aware of the breach, they could have acted far faster and more aggressively in responding to the breach and in assisting victims in redressing harms, including sending notifications to those impacted.

38. Personally Identifiable Information is of high value to criminals. Sensitive information can often be sold on the dark web, with personal information being sold at a price ranging from $40 to $200 and bank details with a price from $50 to $200.[6] The Data Breach exposed PII that is both valuable and

[6] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed November 6, 2024).

highly coveted on underground markets because it can be used to commit identity theft and financial fraud. Identity thieves use such PII to, among other things, gain access to bank accounts, social media accounts, and credit cards. Identity thieves can also use this PII to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government identification cards, or create "synthetic identities." Additionally, identity thieves often wait significant amounts of time—months or even years—to use the PII obtained in data breaches because victims often become less vigilant in monitoring their accounts as time passes, therefore making the PII easier to use without detection.

39. Victims of data breaches are much more likely to become victims of identity fraud than those who have not. Data Breach victims who do experience identity theft often spend hundreds of hours fixing the damage caused by identity thieves.[7] Both Plaintiffs and members of the member class generally have spent hours on end and considerable time and stress in attempting to mitigate the present and future harms caused by the breach. The U.S. Department of Justice's Bureau of Justice Statistics has reported that, even if data thieves have not caused

[7] https://www.marylandattorneygeneral.gov/ID%20Theft%20Documents/Identitytheft.pdf. (last accessed 12/06/2023)

financial harm, data breach victims "reported spending an average of about 7 hours clearing up the issues."[8]

40. The information compromised in the Data Breach—including detailed medical information is much more valuable than the loss of credit card information in a retailer data breach. There, victims can simply close their credit and debit card accounts and potentially even rely on automatic fraud protection offered by their banks. Here, however, the information compromised is much more difficult, if not impossible, for consumers to re-secure after being stolen because it goes to the core of their identity. An individual's medical history and assessments are permanent and are impossible to escape. The loss of all this medical data puts HAWAII RADIOLOGIC patients at additional risk for potential medical fraud and medical identity theft. Indeed, this is especially true for the HAWAII RADIOLOGIC breach where not only was medical and personal information stolen, but also personal private ID information such as state ID numbers, driver's license numbers, and biometric data, which are very difficult or impossible to change.

41. Data breaches involving medical records are not only incredibly costly, they can "also [be] more difficult to detect, taking almost twice as long as

[8] https://bjs.ojp.gov/content/pub/pdf/vit14.pdf. (last accessed Dec. 6, 2023)

normal identity theft."[9] The FTC warns that a thief may use private medical information to, among other things, "see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care"[10] and that this may have far reaching consequences for a victim's ability to access medical care and use insurance benefits.

42. Security standards for businesses storing PII and PHI commonly include, but are not limited to:

a. Maintaining a secure firewall
b. Monitoring for suspicious or unusual traffic on the website
c. Looking for trends in user activity including for unknown or suspicious users
d. Looking at server requests for PII
e. Looking for server requests from VPNs and Tor exit notes
f. Requiring Multi-factor authentication before permitting new IP addresses to access user accounts and PII
g. Structuring a system including design and control to limit user access as necessary including a users access to the account data and PII of other users.

[9] *See What to Know About Medical Identity Theft*, Federal Trade Commission Consumer Information, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited Nov. 6, 2024).
[10] *Id*

43. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity and protection of PII which includes basic security standards applicable to all types of businesses.

44. The FTC recommends that businesses:

a. Identify all connections to the computers where sensitive information is stored.
b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.
c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.
d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.
e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hacker attacks.
f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.
g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall

separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business's network, the transmission should be investigated to make sure it is authorized.

45. As described further below, Defendant owed a duty to safeguard PII and PHI under several statutes, including the Federal Trade Commission Act, 15 U.S.C. § 45 (the "FTC Act") and as a covered entity under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), to ensure that all information it received, maintained, and stored was secure. These statutes were enacted to protect Plaintiff and the Class Members from the type of conduct in

which Defendant engaged, and the resulting harms Defendant proximately caused Plaintiff and the Class Members.

46. Under the FTC Act, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard the PII and PHI of Plaintiffs and Class Members. Under HIPAA, 42 U.S.C. § 1320d, and its implementing regulations, 45 C.F.R. §§ 160, *et seq.*, Defendant had a duty to securely store and maintain the PII and PHI of Plaintiffs and Class Members which was collected in conjunction with receiving medical services.

47. Defendant breached its duty to exercise reasonable care in protecting Plaintiffs and Class Members' PII and PHI by failing to implement and maintain adequate data security measures to safeguard Plaintiffs' and Class Members' sensitive personal information, failing to encrypt or anonymize PII and PHI within its systems and networks, failing to monitor its systems and networks to promptly identify and thwart suspicious activity, failing to delete and purge PII and PHI no longer necessary for its provision of healthcare services to its clients and customers, allowing unmonitored and unrestricted access to unsecured PII and PHI, and allowing (or failing to prevent) unauthorized access to, and exfiltration of, Plaintiffs' and Class Member's confidential and private information. Additionally, Defendant breached its duty by utilizing outdated and ineffectual data security measures which deviated from standard industry best practices at the

time of the Data Breach. Through these actions, Defendant also violated its duties under the FTC Act and HIPAA.

48. Defendant failed to prevent the Data Breach. Had Defendant properly maintained and adequately protected its systems, servers, and networks, the Data Breach would not have occurred.

49. Additionally, the law imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of PII and PHI to Plaintiffs and Class Members so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuses of their private information. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class Members. In so doing, Defendant actually and proximately caused and exacerbated the harm from the Data Breach and the injuries-in-fact of Plaintiffs and Class Members.

50. By Defendant's own admission, on or around August 20, 2024, unauthorized agents gained access to internal information and systems, and Defendant still has not clarified whether the Breach has been fixed.

V. Plaintiffs' and Class Members' Experiences

51. As a precondition for using Defendant's healthcare service, Plaintiffs provided sensitive PII and PHI. Defendant represented to Plaintiff in the

November 5 letter that the breached data included name and date of birth, health insurance subscriber ID, type of exams, and indication for exams provided.

52. Plaintiffs have taken reasonable steps to maintain the confidentiality of her PII. They relied upon HAWAII RADIOLOGIC's representations, experience, and sophistication to keep their information secure and confidential.

53. As a result of the data breach, Plaintiffs were forced to take measures to mitigate the harm, including spending time monitoring their credit and financial accounts, researching the Data Breach, and researching and taking steps to prevent and mitigate the likelihood of identity theft.

54. Plaintiff RAMISCAL lives in Hawai'i and has been a patient of HAWAII RADIOLOGIC. As a result of the Data Breach, Plaintiff RAMISCAL suffered actual injuries including: (a) paying money to HAWAII RADIOLOGIC for services, which Plaintiff would not have done had HAWAII RADIOLOGIC disclosed that it lacked data security practices adequate to safeguard Plaintiff's PII and PHI from theft; (b) damages to and diminution in the value of Plaintiff's PII and PHI—property that Plaintiff entrusted to HAWAII RADIOLOGIC as a condition of receiving its services; (c) loss and invasion of Plaintiff' privacy; and (d) injuries arising from the increased risk of fraud and identity theft, including the cost of taking reasonable identity theft protection measures, which will continue for years.

55. Plaintiff ARKIN lives in Hawai'i and has been a patient of HAWAII RADIOLOGIC. As a result of the Data Breach, Plaintiff ARKIN suffered all the same injuries enumerated in the paragraph above, and in addition, Plaintiff ARKIN has also suffered injuries resulting from delays in the delivery of radiologic images from HAWAII RADIOLOGIC caused by the Data Breach. Specifically, ARKIN explained that at the time of the Data Breach, she relied exclusively on Defendant for radiologic imaging services which were necessary for the treatment of a medical condition. Thus, when HAWAII RADIOLOGIC shut down its services for the entire month of September 2024 as a security measure against the Data Breach, this resulted in a three-week delay in the delivery of radiologic images necessary to ascertain the results of the treatment of Plaintiff's medical condition. As a result of this three-week delay, Plaintiff had to cancel three appointments with her surgeon, which were of vital importance to the treatment of her medical condition. Thus, for Plaintiff ARKIN, the Data Breach also took a detrimental toll on her mental wellbeing by delaying the highly anticipated results of treatment for a serious medical condition.

CLASS ACTION ALLEGATIONS

56. Plaintiffs bring this action as a class action pursuant to Rules 23(a) and 23(b)(1)-(3) of the Federal Rules of Civil Procedure, on behalf of themselves and a Nationwide Class defined as follows:

All persons in the United States whose PII/PHI were compromised by the Data Breach that occurred on HAWAII RADIOLOGIC'S computer networks in or around August 2024.

57. Excluded from the Nationwide Class are governmental entities, Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, affiliates, legal representatives, employees, coconspirators, successors, subsidiaries, and assigns. Also excluded from the Nationwide Class are any judges, justices, or judicial officers presiding over this matter and the members of their immediate families and judicial staff.

58. This action is brought and may be properly maintained as a class action pursuant to Rule 23. This action satisfies the requirements of Rule 23, including numerosity, commonality, typicality, adequacy, predominance, and superiority.

59. **Numerosity.** The Nationwide Class are so numerous that the individual joinder of all members is impracticable. While the Nationwide Class exact number are currently unknown and can only be ascertained through appropriate discovery, Plaintiff, on information and belief, allege that the Nationwide Class includes at least 23,205 members based on data provided by the United States Department of Health and Human Services.[11]

[11] *See supra* n.1.

60. **Commonality.** Common legal and factual questions exist that predominate over any questions affecting only individual Nationwide Class Members. These common questions, which do not vary among Nationwide Class Members and which may be determined without reference to any Nationwide Class Member's individual circumstances, include, but are not limited to:

a. Whether Defendant knew or should have known that its systems were vulnerable to unauthorized access;
b. Whether Defendant failed to take adequate and reasonable measures to ensure its data systems were protected;
c. Whether Defendant failed to take available steps to prevent and stop the breach from happening or mitigating the risk of a long-term breach;
d. Whether Defendant unreasonably delayed in notifying patients once they discovered suspicious activity.
e. Whether Defendant unreasonably delayed in notifying patients they had confirmed a breach of their data systems.
f. Whether Defendant unreasonably delayed in notifying victims once Defendant had concluded its investigation.
g. Whether Defendant owed a legal duty to Plaintiffs and Class Members to protect their PII and PHI;
h. Whether Defendant breached any duty to protect the personal information of Plaintiffs and Class Members by failing to exercise due care in protecting their PII and PHI;
i. Whether Plaintiffs and Class Members are entitled to actual, statutory, or other forms of damages and other monetary relief; and,

j. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief or restitution.

61. **Typicality.** Plaintiffs' claims are typical of other Class Members' claims because Plaintiffs and Class Members were subjected to the same allegedly unlawful conduct and damaged in the same way.

62. **Adequacy of Representation.** Plaintiffs are an adequate Nationwide Class representative because they are Nationwide Class Members, and their interests do not conflict with the Nationwide Class' interests. Plaintiffs retained counsel who are competent and experienced in class action and data breach litigation. Plaintiffs and their counsel intend to prosecute this action vigorously for the Nationwide Class' benefit and will fairly and adequately protect their interests.

63. **Predominance and Superiority.** The Nationwide Class can be properly maintained because the above common questions of law and fact predominate over any questions affecting individual Nationwide Class Members. A class action is also superior to other available methods for the fair and efficient adjudication of this litigation because individual litigation of each Nationwide Class member's claim is impracticable. Even if each Nationwide Class member could afford individual litigation, the court system could not. It would be unduly burdensome if thousands of individual cases proceed. Individual litigation also presents the potential for inconsistent or contradictory judgments, the prospect of

a race to the courthouse, and the risk of an inequitable allocation of recovery among those with equally meritorious claims. Individual litigation would increase the expense and delay to all parties and the courts because it requires individual resolution of common legal and factual questions. By contrast, the class-action device presents far fewer management difficulties and provides the benefit of a single adjudication, economies of scale, and comprehensive supervision by a single court.

64. **Declaratory and Injunctive Relief.** The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members that would establish incompatible standards of conduct for Defendant. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other Class Members and impair their interests. Defendant has acted and/or refused to act on grounds generally applicable to the Class, making final injunctive relief or corresponding declaratory relief appropriate.

CLAIMS FOR RELIEF

Count 1
Negligence
On behalf of Plaintiffs and the Nationwide Class

65. Plaintiffs incorporate by reference and reallege each and every allegation above as though fully set forth herein.

66. Plaintiffs were required to provide PII and PHI as a precondition for using the HAWAII RADIOLOGIC's healthcare services.

67. Plaintiff and Class Members entrusted their PII and PHI to HAWAII RADIOLOGIC with the understanding that HAWAII RADIOLOGIC would safeguard their PII and PHI.

68. In its written privacy policies, HAWAII RADIOLOGIC committed to taking reasonable steps to protecting patient PHI and PII. HAWAII RADIOLOGIC also acknowledged its obligation to abide by privacy regulations including HIPAA and committed to limit the degree to which this sensitive information was shared with other parties.[12]

69. HAWAII RADIOLOGIC specifically acknowledged and represented to consumers, including Plaintiffs and Class Members, that it was "required by law to maintain the privacy of your health information."[13]

70. However, it appears that more than 23,205 patients (including Plaintiffs) had sensitive data exfiltrated by hackers without their knowledge or consent.

[12] FAQ, HAWAII RADIOLOGIC ASSOCIATES, https://www.hirad.com/faq/, (last visited November 23, 2024).
[13] Notice of Privacy Practices, HAWAII RADIOLOGIC ASSOCIATES, https://www.hirad.com/privacy-policy/#:~:text=We%20may%20use%20or%20disclose,the%20purposes%20of%20a%20consultation, (last visited November 23, 2024).

71. HAWAII RADIOLOGIC did not take reasonable and appropriate safeguards to protect Plaintiff and Class Members' PII.

72. HAWAII RADIOLOGIC had full knowledge of the sensitivity of the PII that it stored and the types of harm that Plaintiffs and Class Members could and would suffer if that PII were wrongfully disclosed.

73. HAWAII RADIOLOGIC violated its duty to implement and maintain reasonable security procedures and practices. That duty includes, among other things, designing, maintaining, and testing HAWAII RADIOLOGIC's information security controls sufficiently rigorously to ensure that PII and PHI in its possession was adequately secured by, for example, encrypting sensitive personal information, installing effective intrusion detection systems and monitoring mechanisms, using access controls to limit access to sensitive data, regularly testing for security weaknesses and failures, failing to notify customers of the breach in a timely manner, and failing to remedy the continuing harm by unreasonably delaying notifying specific victims who were harmed.

74. HAWAII RADIOLOGIC's duty of care arose from, among other things,

a. HAWAII RADIOLOGIC's exclusive ability (and Class Members' inability) to ensure that its systems were sufficient to protect against the foreseeable risk that a data breach could occur;

b. Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, failing to adopt reasonable data security measures;

c. HIPAA, 42 U.S.C. § 1320d, and its implementing regulations, 45 C.F.R. §§ 160, *et seq.*, under which Defendant had a duty to securely store and maintain the PII and PHI of Plaintiffs and Class Members, which was collected in conjunction with receiving healthcare services. Additionally, the HIPPA Breach Notification Rule, 45 C.F.R. § 164.400-414, required Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

d. HAWAII RADIOLOGIC's common law duties to adopt reasonable data security measures to protect customer PII and to act as a reasonable and prudent person under the same or similar circumstances would act;

75. These statutes—the FTC Act and HIPAA—were enacted to protect Plaintiffs and the Class Members from the type of wrongful conduct in which Defendant engaged.

76. HAWAII RADIOLOGIC's violation of the FTC Act and HIPAA constitutes negligence per se for purposes of establishing the duty and breach elements of Plaintiffs' negligence claim. Those statutes were designed to protect a

group to which Plaintiffs belong and to prevent the types of harm that resulted from the Data Breach.

77. Plaintiffs and Class Members were the foreseeable victims of HAWAII RADIOLOGIC's inadequate data security. HAWAII RADIOLOGIC knew that a breach of its systems could and would cause harm to Plaintiffs and Class Members.

78. HAWAII RADIOLOGIC's conduct created a foreseeable risk of harm to Plaintiffs and Class Members. HAWAII RADIOLOGIC's conduct included its failure to adequately mitigate harm through negligently failing to inform patients and victims of the breach for over two months after the purported first discovery of suspicious activity.

79. HAWAII RADIOLOGIC knew or should have known of the inherent risks in collecting and storing massive amounts of PII and PHI, the importance of providing adequate data security over that PII and PHI, and the frequent cyberattacks within the medical industry.

80. HAWAII RADIOLOGIC, through its actions and inactions, breached its duty owed to Plaintiffs and Class Members by failing to exercise reasonable care in safeguarding their PII and PHI while it was in their possession and control. HAWAII RADIOLOGIC breached its duty by, among other things, its failure to adopt reasonable data security practices and its failure to adopt reasonable security

and notification practices in the result in a breach including monitoring internal systems and sending notifications to affected victims. HAWAII RADIOLOGIC did not provide sufficient information to patients either while the breach was occurring or immediately afterwards. For months, it downplayed the data breach publicly whilst knowing patient data was compromised.

81. HAWAII RADIOLOGIC inadequately safeguarded consumers' PII and PHI in breach of standard industry rules, regulations, and best practices at the time of the Data Breach.

82. But for HAWAII RADIOLOGIC's breach of its duty to adequately protect Class Members' PII and PHI, Class Members' PII and PHI would not have been stolen.

83. There is a temporal and close causal connection between HAWAII RADIOLOGIC's failure to implement adequate data security measures and notification practices, the Data Breach, and the harms suffered by Plaintiffs and Class Members.

84. As a result of HAWAII RADIOLOGIC's negligence, Plaintiffs and Class Members suffered and will continue to suffer the damages alleged herein.

85. Plaintiffs and Class Members are entitled to all forms of monetary compensation set forth herein, including monetary payments to provide adequate

identity protection services. Plaintiffs and Class Members are also entitled to the injunctive relief sought herein.

Count 2
Breach of Implied Contract
On behalf of Plaintiffs and the Nationwide Class

86. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth above and incorporate them by reference as though set forth in full here.

87. Plaintiffs and Class Members entered into an implied contract with HAWAII RADIOLOGIC when they entrusted Defendant with their PII and PHI.

88. As part of these transactions, HAWAII RADIOLOGIC agreed to safeguard and protect the PII of Plaintiffs and Class Members and to timely and accurately notify them if their PII or PHI was breached or compromised.

89. Plaintiffs and Class Members entered into the implied contracts with the reasonable expectation that HAWAII RADIOLOGIC's data security practices and policies were reasonable and consistent with the legal requirements and industry standards. Plaintiffs and Class Members believed that HAWAII RADIOLOGIC would use part of the monies paid to HAWAII RADIOLOGIC under the implied contracts or the monies obtained from the benefits derived from the PII and PHI they provided to fund proper and reasonable data security practices.

90. Plaintiffs and Class Members would not have provided and entrusted their PII and PHI to HAWAII RADIOLOGIC or would have paid less for HAWAII RADIOLOGIC's products or services in the absence of the implied contract or implied terms between them and HAWAII RADIOLOGIC. The safeguarding of the PII of Plaintiffs and Class Members was critical to realize the intent of the parties.

91. Plaintiffs and Class members fully performed their obligations under the implied contracts with HAWAII RADIOLOGIC.

92. HAWAII RADIOLOGIC breached its implied contracts with Plaintiffs and Class Members to protect their PII when it (1) failed to take reasonable steps to use safe and secure systems to protect that information; (2) disclosed that information to unauthorized third parties and; (3) failed to notify Plaintiffs and Class Members in a reasonably timely manner.

93. As a direct and proximate result of HAWAII RADIOLOGIC's breach of implied contract, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the

confidentiality of the stolen PII and PHI; illegal sale of the compromised PII and PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII PHI; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the HAWAII RADIOLOGIC Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

94. As a direct and proximate result of the breach, Plaintiffs are entitled to relief as set forth herein.

Count 3
Unjust Enrichment
On behalf of Plaintiffs and the Nationwide Class

95. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth above and incorporate them by reference as though set forth in full herein.

96. Plaintiffs and Class Members entered into an implied contract with HAWAII RADIOLOGIC when they obtained products or services from HAWAII

RADIOLOGIC, joined a healthcare program, or otherwise provided PII or PHI to HAWAII RADIOLOGIC.

97. As part of these transactions, HAWAII RADIOLOGIC agreed to safeguard and protect the PII and PHI of Plaintiffs and Class Members and to timely and accurately notify them if their PII was breached or compromised.

98. Plaintiffs and Class Members entered into the implied contracts with the reasonable expectation that HAWAII RADIOLOGIC's data security practices and policies were reasonable and consistent with legal requirements and industry standards. Plaintiffs and Class Members believed that HAWAII RADIOLOGIC would use part of the monies paid to HAWAII RADIOLOGIC under the implied contracts or the monies obtained from the benefits derived from the PII and PHI they provided to fund proper and reasonable data security practices.

99. Plaintiffs and Class Members would not have provided and entrusted their PII and PHI to HAWAII RADIOLOGIC or would have paid less for HAWAII RADIOLOGIC products or services in the absence of the implied contract or implied terms between them and HAWAII RADIOLOGIC. The safeguarding of the PII and PHI of Plaintiffs and Class Members was critical to realize the intent of the parties.

100. Plaintiffs and Class members fully performed their obligations under the implied contracts with HAWAII RADIOLOGIC.

101. HAWAII RADIOLOGIC breached its implied contracts with Plaintiffs and Class Members to protect their PII and PHI when it (1) failed to take reasonable steps to use safe and secure systems to protect that information; (2) disclosed that information to unauthorized third parties and; (3) failed to notify Plaintiffs and Class Members in a timely and reasonable fashion.

102. As a direct and proximate result of HAWAII RADIOLOGIC's breach of implied contract, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII and PHI; illegal sale of the compromised PII and PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII and PHI; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures

because of HAWAII RADIOLOGIC's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class set forth herein, respectfully request the following relief:

A. That the Court certify this action as a class action and appoint Plaintiffs and their counsel to represent the Class;

B. That the Court grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein and directing Defendant to adequately safeguard the PII of Plaintiffs and the Class by implementing improved security controls;

C. That the Court award compensatory, consequential, and general damages, including nominal damages as appropriate, as allowed by law in an amount to be determined at trial;

D. That the Court award statutory or punitive damages as allowed by law in an amount to be determined at trial;

E. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendant as a result of Defendant's unlawful acts, omissions, and practices;

F. That the Court award to Plaintiffs and Class Members the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses; and

G. That the Court award pre- and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial on all claims so triable.

Dated: Honolulu, HI, ____November 26, 2024_____.

_____*/s/* Janice D. Heidt_____
Janice D. Heidt
Richard Turbin
Amber L. Schubert

Attorneys for Plaintiff and the Proposed Class